Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-16. (Canceled)

17. (Currently amended) An optical disk playing system comprising:

a plurality of downloadable media content provided on one or more computing devices distributed on a network, each downloadable media content having an added private key ~~and is~~ associated with at least one stored media content;

an optical disk comprising

a first stored media content that is played in coordination with the downloadable media content associated with the first stored media content, and

a public key ~~which is used~~ to verify the authenticity of each of the downloadable media content in cooperation with the private key of the downloadable media content before the first stored media content is played in coordination with the associated downloadable media content,

wherein the authenticity of the downloadable media content is verified independent of the authenticity of the one or more computing devices on which the downloadable media content is provided.

18. (Previously presented) The optical disk playing system according to claim 17, wherein the public key is stored in a BCA (Burst Cutting Area) zone of the optical disk.

19. (Previously presented) The optical disk playing system according to claim 17, wherein the public key is stored in a media content zone of the optical disk.

20. (Currently amended) An optical disk player comprising:

an optical disk driver unit to read-out stored media content and a public key provided on an optical disk on which the stored media content is stored, the public key is used for authenticating external media content having an added private key;

a network interface to download one or more external media content, each external media content having ~~an~~ the added private key ~~and is~~ associated with ~~the~~ at least one stored media content, the one or more external media content provided on one or more computing devices distributed on a network; and

a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk and the added private key of the downloaded external media content before the stored media content is played in coordination with the associated downloaded external media content,

wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided.

21. (Previously presented) The optical disk player according to claim 20, wherein the control system detects whether the downloaded external media content is integral before verification, wherein said verification will not be executed if the downloaded external media content is detected to not be integral.

22. (Previously presented) The optical disk player according to claim 20, wherein the downloaded external media content is an application program.

23. (Previously presented) The optical disk player according to claim 22, wherein the application program is a JAVA language application program.

24. (Currently amended) The optical disk player according to claim 20, wherein the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk ~~and a~~ corresponding to the added private key encrypted in the downloaded external media content.

25. (Currently amended) A method for playing an optical disk, comprising acts of:

reading-out stored media content and a public key provided on an optical disk on which the stored media content is stored, the public key is used to verify authenticity of external media content having a private key;

downloading one or more external media content including ~~a~~ the private key, each

external media content being associated with the read-out stored media content;

verifying the authenticity of each of the downloaded external media content using the public key read-out from the optical disk and the private key of the downloaded external media content before allowing the read-out stored media content to be played in coordination with the one or more associated downloaded external media content,

wherein the authenticity of the external media content is verified independent of the authenticity of one or more computing devices on which the external media content is provided.

26. (Previously presented) The method according to claim 25, further comprising acts of:

detecting if the downloaded external media content is integral; and

executing the verifying act only if the downloaded external media content is detected to be integral.

27. (Previously presented) The method according to claim 25, wherein the coordination between the read-out stored media content and the downloaded external media content will not be established if the downloaded external media content is not authenticated.

28. (Previously presented) The method according to claim 27, wherein the coordination between the read-out stored media content and downloaded external media content will be established if the downloaded external media content is authenticated.

29. (Previously presented) The method according to claim 25, wherein the downloaded external media content is an application program.

30. (Previously presented) The method according to claim 29, wherein the application program is a JAVA language application program.

31. (Currently amended) The method according to claim 25, wherein verifying the authenticity of the downloaded external media content comprises an act of performing asymmetric cryptography using the public key read-out from the optical disk ~~and a~~ corresponding to the private key ~~of~~ encrypted in the downloaded external media content.

32. (Currently amended) The method according to claim 25, wherein the optical disk comprises digital information stored thereon, the stored digital information comprising network address information that is used to download the external media content and ~~a~~ the public key that is used to verify the authenticity of the downloaded external media content before playing the stored media content in coordination with the external media content.